CYLANCE CONSULTING

Industrial Control System Security Assessment

Identify and Mitigate Risks in Your ICS Environment

Benefits

- Raise awareness and facilitate discussions on cybersecurity in regards to control systems
- Highlight vulnerabilities and remediation strategies for the ICS environment
- Create remediation strategies balancing risk and return
- Identify areas of strength and best practices being followed within the organization
- Improve the organization's risk management and decision-making process
- Develop a systematic and repeatable approach to assessing the security posture of ICS systems

The nation's critical infrastructure experienced a 20 percent increase in cyber incidents.

Source: Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) Report, FY2015

CYLANCE

+1-877-97DEFEND
proservices@cylance.com
www.cylance.com/consulting
18201 Von Karman Avenue
Suite 700, Irvine, CA 92612

Industrial Control Systems (ICS) were originally built as stand-alone systems that were not interconnected and contained little in the way of security protections. But, they are now being targeted by the same cybersecurity threats that typical corporate networks face, forcing organizations to develop security strategies to protect assets and limit risk.

While many considerations must be taken when addressing the fragile nature of ICS environments, an ICS Security Assessment can aid in **identifying and remediating vulnerabilities** that would allow an attacker to disrupt or take control of the system. Based on the results, the assessment can help **guide decisions to enhance the organization's cybersecurity posture.**

Service Overview

Cylance® Consulting's globally-recognized ICS security experts will work closely with organizations to evaluate the security practices of the industrial control system environment. The ICS Assessment is centered on providing context in regards to the potential business impact of cyberthreats, the vulnerability of the systems to attack, and whether there is any evidence to indicate a compromise has already occurred.

The assessment provides an effective means to identify the highest priority security concerns and recommendations for the control system environment. The primary categories for the assessment include:

- Network Architecture Review
- Policy and Procedures Review
- Vulnerability Assessment
- Compromise Assessment

Information is collected about the organization's security practices, policies, and procedures through survey responses, staff interviews, tools, company documentation, and site walk downs.

Deliverables

The information obtained from the assessment is used to provide the organization with:

- A risk profile that addresses impact, threat, vulnerability, probability, and countermeasures
- A prioritized road map for remediating security concerns

Identify weaknesses and develop actionable recommendations to mitigate the risks in your ICS environment. Contact Cylance Consulting or your technology provider to discuss your needs.